US006499106B1

(12) **United States Patent**
Yaegashi et al.

(10) **Patent No.: US 6,499,106 B1**
(45) **Date of Patent: Dec. 24, 2002**

(54) **METHOD AND APPARATUS FOR SECURE DISTRIBUTION OF INFORMATION RECORDED OF FIXED MEDIA**

(75) Inventors: **Akira Yaegashi**, San Diego, CA (US); **Henry Theo F. Guico**, San Diego, CA (US)

(73) Assignees: **Sony Corporation**, Tokyo (JP); **Sony Electronics Inc.**, Parkridge, NJ (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/247,572**

(22) Filed: **Jan. 15, 1999**

(51) **Int. Cl.**[7] **G06F 12/14**

(52) **U.S. Cl.** **713/193**

(58) **Field of Search** 713/193, 168, 713/200, 201; 380/277, 278; 705/52, 51

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,405,829 A		9/1983	Rivest et al.	178/22.1
4,932,054 A		6/1990	Chou et al.	380/4
4,977,594 A		12/1990	Shear	380/4
5,136,646 A		8/1992	Haber et al.	380/49
5,136,647 A		8/1992	Haber et al.	380/49
5,247,575 A		9/1993	Sprague et al.	380/9
5,771,291 A	*	6/1998	Newton et al.	380/277
6,088,451 A	*	7/2000	He et al.	380/255
6,104,679 A	*	8/2000	Sollish	369/53.21
6,134,324 A	*	10/2000	Bohannon et al.	705/52
6,192,405 B1	*	2/2001	Bunnell	709/202

FOREIGN PATENT DOCUMENTS

WO	WO 93/01550	1/1993

OTHER PUBLICATIONS

U.S. application Ser. No. 09/245,107, filed Jan. 15, 1999.
Schneier, B., "Applied Cryptography–Protocols, Algorithms, and Source Code in C", Copyright 1994, ISBN 0–471–59756–2.
Diffie, W., et al., "IEEE Transactions on Information Theory–New Directions", Nov. 1976, vol. IT–22, No. 6, pp. 644–654.

* cited by examiner

Primary Examiner—Matthew Smithers
(74) *Attorney, Agent, or Firm*—Sony Electronics Inc.

(57) **ABSTRACT**

A central access control system creates distribution CDs using an embedded data encryption process. A disc ID is also encrypted and recorded on each disc of each set of distribution CDs. The central access control system records the disc IDs and a remote location access rights list (ARL). A list of unique remote location IDs are also stored. The distribution CDs are delivered to one or more remote locations equipped with an information access system that includes its unique remote location ID, a CD reader with an embedded decryption system, and a communication link to the central access control system. The information access system can send the disc ID and its unique remote location ID as an access request to the central access control system. If the access control system is able to verify and grant the request, a unique decryption key will be sent to access the particular distribution CD currently contained in the information access system. The unique remote location ID of each information access system is a public encryption key and the central access control system encrypts the distribution CD's decryption key using the requesting information access system's public key. If the central access control system is unable to verify or grant the request, an attempted security breach alert is triggered.

19 Claims, 3 Drawing Sheets